Here's a **comprehensive, bullet-point, sentence-by-sentence breakdown** of the document **"25. Product Lifecycle"**, fully aligned with your CompTIA A+ 1102 exam preparation framework:

**🧠 Concept Overview**

The **product lifecycle** is the timeline a software product (like Windows OS) follows from its release to the point it's no longer supported. Understanding this helps IT professionals plan for updates, avoid security vulnerabilities, and stay compliant.

**📘 Sentence-by-Sentence Breakdown**

**🔹 Introduction to Product Lifecycle**

* Every new **product or OS** follows a **defined lifecycle**.
* Some manufacturers **clearly state** their lifecycle policies so users know **what support to expect**.
* Others do not offer that level of transparency.

**🔹 Microsoft's Lifecycle Transparency**

* Microsoft is known for being **transparent** about its **product lifecycle policies**.
* For each version of Windows, there are **two types of support**:
  + **Mainstream Support**
  + **Extended Support**

**🔹 Mainstream vs. Extended Support**

* **Mainstream Support**: Usually lasts **5 years**; includes feature updates, bug fixes, and security patches.
* **Extended Support**: Adds another **3–5 years** of **security updates only** (no new features).

**🔹 End of Life (EOL) and Legacy Systems**

* When both support phases end, the OS reaches **end of life (EOL)**.
* EOL software becomes a **legacy operating system**—a product that is no longer **supported and is vulnerable**.
  + No more software patches or bugs for that OS.
* Legacy OS examples: **Windows XP**, still used in special environments.

**🔹 Case Study: Windows XP**

* Windows XP support ended in **2015**.
* Still found in use, especially in **ICS and SCADA systems** (industrial control systems).
  + An attacker can’t physically get to ICS and SCADA systems due to it not being connected to the internet, so its relatively safe.
* XP machines **can still run**, but **won’t receive no support or updates**.
  + So if a hacker or attacker discovers some kind of vulnerability in Windows XP and numerous ones have been discovered since the end of life, those now are open vulnerabilities that will never get solved.
  + So if your running Windows XP you are extremely vulnerable and that you should never be connected to the internet because people can hack you immediately.
* Any discovered vulnerabilities will **never be patched**.
* XP systems **must not be connected to the internet**—extremely vulnerable.

**🔹 Why Legacy Systems Persist**

* XP used in critical infrastructure because **upgrading is expensive** (factories may need full hardware overhauls).
* If kept **offline**, such systems may still operate **safely**.

**🔹 Modern OS Lifecycle Examples**

* **Windows 10 Home/Pro**: Released in **2015**, retires in **2025** = 10 years total.
* **Windows 11 21H2**: Released in **2021**, retires **October 2023** (shorter lifecycle).
  + **The current version of windows 11 will reach its EOL and there’ll be a new version of Windows 11 that will then get an additional two to three years of support**.

**🔹 Lifecycle Variability**

* Different **Windows versions** (even within Windows 11) have **independent timelines**.
* Versions with heavy **corporate adoption** may receive **longer support**.
  + Give additional support to its larger main stream customers.

**🔹 Corporate vs. Consumer Support**

* Microsoft extends support based on **enterprise needs**.
* Home users benefit from **the same patches** created for businesses.

**🔹 Feature Updates**

* Released every **6 to 12 months**.
* Add **new functions** to existing Windows versions.
* Does **not change OS version**, but enhance capabilities.

**🔹 System Requirements and PC Health Check**

* Feature updates **rarely change** base hardware requirements.
* Always use **PC Health Check** to ensure your system supports updates.

**🔹 Growing Storage Needs**

* Earlier Windows 10 builds required **20 GB** of space.
* Newer versions now need **32 GB** due to accumulated features.

**🔹 Summary and Final Advice**

* All OS products have a **finite lifecycle** (typically 2–5 years).
* Microsoft ensures at least **5 years mainstream** and up to **10+ years extended support**.
* After EOL, systems receive **no patches or fixes**, creating **security liabilities**.
* Upgrade legacy systems to **supported versions** to maintain security and functionality.

**✅ Exam Relevance (CompTIA A+ 1102)**

**Topics Covered:**

* **1.4** — Operating system installation and upgrade considerations.
* **1.6** — OS maintenance and feature updates.
* **4.1** — Security risks from unsupported OS versions.

**Key Terms to Know:**

* **Mainstream Support**
* **Extended Support**
* **End of Life (EOL)**
* **Legacy Operating System**
* **ICS/SCADA Systems**
* **PC Health Check**
* **Feature Updates**

**🛠 Real-Life Scenario**

A city’s power grid uses SCADA systems controlled by a machine running Windows XP. While it can’t be updated due to proprietary software compatibility, it’s kept offline and isolated from the internet to minimize risk. The IT department documents the system, monitors physical access, and plans for a long-term upgrade.

**📌 Exam Inclusion Notification**

✅ This topic **is included** in the CompTIA A+ 1102 exam. You are expected to understand the **lifecycle phases** of operating systems, the implications of using unsupported versions, and how to plan upgrades appropriately.